

RECEIVED

CENTRAL FAX CENTER

MAY 23 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Lane Lee et al.

Application No.: 09/939,896 Filing Date: August 27, 2001

Examiner: Bradley B. BAYAT Group Art Unit: 3621

Docket No.: M-12042 US Confirmation No.

Irvine, California
May 23, 2008

Via Facsimile to (571) 273-8300

Mail Stop : Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that the following documents are being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below:

- 1) Transmittal of Appellant's Opening Appeal Brief (Amended) (1 page); and
- 2) Appellant's Opening Brief (10 pages)

Dated: May 23, 2008

Saundra L Carr

Saundra L. Carr

Number of pages (including this sheet): 12

MacPherson Kwok Chen & Heid LLP
2033 Gateway Place, Ste. 400
San Jose, CA 95110

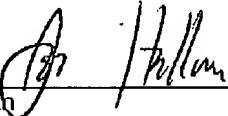
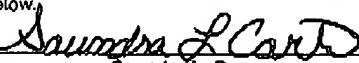
Telephone: (949) 752-7040
Fax: (408) 392-9262 and (949) 752-7049

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP
2033 Gateway Place, Ste. 400
SAN JOSE, CA 95110
(949) 752-7040
FAX (408) 392-9262

Fax to USPTO

RECEIVED
CENTRAL FAX CENTER

MAY 23 2008

TRANSMITTAL OF APPELLANT'S OPENING APPEAL BRIEF (AMENDED)		Docket No. M-12042 US
In re Application of: Lane Lee et al.		
Application No. 09/939,896	Filing Date August 27, 2001	Examiner Bradley B. BAYAT
Group Art Unit 3621		
Invention: Revocation Method and Apparatus for Secure Content		
TO THE COMMISSIONER OF PATENTS:		
Transmitted herewith is the Appellant's Opening Appeal Brief in response to the Notice of Non-Compliant Appeal Brief dated February 25, 2008.		
The fee for filing this Appeal Brief is <u>PAID</u> .		
<input type="checkbox"/> Large Entity <input checked="" type="checkbox"/> Small Entity		
<input checked="" type="checkbox"/> Applicant(s) Petitions for an Extension of Time for two months (2):		
The fee for the extension of time is <u>\$230.00</u> .		
<input checked="" type="checkbox"/> Kindly charge \$230.00 to Deposit Account No. <u>50-2257</u> .		
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. <u>50-2257</u> .		
 Jonathan W. Hallman Attorney Reg. No. : 42,622 MacPherson Kwok Chen & Heid LLP 2033 Gateway Place, Ste. 400 San Jose, CA 95110 (408) 392-9250 Facsimile: (408) 392-9262		Dated: <u>5/23/08</u>
CERTIFICATE OF FACSIMILE TRANSMISSION		
I hereby certify that this correspondence is being facsimile transmitted to the U.S. Patent and Trademark Office, Mail Box: Appeal Brief, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.		
Dated: May 23, 2008	Signature:  Saundra L. Carr	
05/27/2008 VBUI11 00000027 502257 09939896 01 FC:2252 230.00 DA		

TRANSMITTAL OF AMENDED APPEAL BRIEF IN RESPONSE TO NOTICE NONCOMPLIANT BRIEF.DOC

RECEIVED
CENTRAL FAX CENTER

MAY 23 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Lane Lee, et al.

Application No. 09/939,896

Filing Date: 08/27/2001

For: Revocation Method and Apparatus for
Secure Content

Examiner: Bradley B. Bayat

Art Unit: 3621

Confirmation No. 4074

Attorney Docket No.: M-12042 US

APPELLANTS' OPENING BRIEF

Real Party In Interest

The real party in interest is DPHI Acquisitions, Inc., the present assignee of US Application No. 09//939,896.

Related Appeals and Interferences

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1 – 35, and 41 – 43 are cancelled.

Claims 36 – 40 are pending and are finally rejected by the Office Action dated February 23, 2007.

The rejection of claims 36 – 40 is appealed.

Status of Amendments

An amendment was filed and entered in the response dated November 28, 2006. An amendment under 37 CFR § 41.33 is concurrently filed with this appeal brief to amend claim 39 so as to address the minor informality noted by the Examiner. No other amendments have been filed subsequent to the Office Action dated February 23, 2007.

Summary of Claimed Subject Matter

The claimed subject matter is directed to a digital rights management (DRM) technique. In general, it is conventional in a DRM implementation to authenticate a party before access to content is granted. For example, content providers provide digital certificates to content users so that they become authorized to access protected content. In such a DRM implementation, a user at a host device such as a personal computer may obtain a digital certificate that is then provided to a storage engine controlling access to protected content stored on a storage medium. The authentication process comprises verifying a digital signature provided by the content provider that is contained within the digital certificate. Once the signature is authorized, the user is authenticated and may proceed to access the protected content.

However, because authentication schemes involve the use of credentials that may become compromised, there is another layer of protection commonly available in conventional DRM schemes. That layer would be the revocation process, which follows authentication. In other words, even though a user may possess valid (authenticated) credentials, if that user is identified by a revocation list, the user is denied access to the protected content. This revocation process follows authentication and is thus performed as an initial handshaking routine between the host device and the storage engine. As will be discussed further, the primary Nonaka reference (U.S. Publication No. 2003/0046238) cited against the pending claims in this matter discloses such a conventional "all or nothing" revocation scheme. These schemes are "all or nothing" because a user is either revoked or not following authentication. In other words, the revocation applies to all content that would otherwise be accessible following authentication.

The Applicants disclose and claim a very different revocation scheme. Rather than be "all or nothing" as disclosed in the conventional Nonaka reference, Applicants disclose a DRM implementation having a file-by-file revocation technique. Such a revocation scheme is much more granular and flexible than the conventional all or nothing approach. Claim 36 recites such a technique that includes the act of "receiving at a storage engine a certificate from

the host device, the certificate containing a digital signature." Support for this act is shown with regard to element 612 of Figure 6 and the supporting discussion on page 29, lines 13-25. Claim 36 further recites an act of "authenticating the digital signature." Support for this act is discussed with regard to element 614 of Figure 6 and the supporting discussion on page 29, lines 13-25. Claim 36 further recites an act of "establishing a secure session by transmitting a session key to the host device." Support for this act is shown with regard to element 622 of Figure 6 and the supporting discussion on page 29, line 26 through page 30, line 2. Given this establishment of a secure session, claim 36 further recites the act of "during the secure session: receiving at the storage engine a file request from the host device, the file request being directed to a file stored on a storage medium accessible to the storage engine." Support for this limitation is shown with regard to block 712 of Figure 7c and the supporting discussion on page 31, lines 15-22.

Given this supporting context of claim 36, the file-by-file revocation scheme is then recited in claim 36 through the acts of "reading a revocation list associated with the file from the storage medium, the revocation list containing at least one rule, the at least one rule associating data in the revocation list with data in the certificate; applying the at least one rule on the data in the revocation list and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request." Support for these file-by-file revocation acts are given by page 31, line 20 through page 32, line 5. For example, "reading a revocation list associated with the file from the storage medium" is described on page 31, lines 20-21, where the Applicants note that "a revocation list is evaluated upon a file access." As stated on page 32, lines 24-28, Applicants note that a revocation list may be made up of a list of "revocation nodes," where each revocation node is made up of a list of clause nodes and a rule of how to combine the clauses to determine a revocation for the node. Each clause node "is made up of a set of data and functions that define how to apply the data and evaluate them against the fields in a received CKDRM certificate." Thus, Applicants have written support for the limitation of "the revocation list containing at least one rule, the at least one rule associating data in the

revocation list with data in the certificate." As set forth on page 33, lines 1-6, if the evaluation of the revocation list is negative, the host is denied access to the file. Accordingly, Applicants have written support for the claim element of "applying the at least one rule on the data in the revocation list and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request." An example structure for rules in the revocation list (the rules also being denoted as "revocation nodes" as noted above) is shown in Table 26 on page 33.

Grounds of Rejection to Be Reviewed on Appeal

- 1) Whether, under 35 U.S.C § 112, claim 39 is indefinite
- 2) Whether, under 35 U.S.C. § 102(e), claims 36 – 40 are anticipated by U.S. Publication No. 2003/0046238 to Nonaka.

Argument

1) Rejection under 35 U.S.C. 112

Claim 39:

The enclosed Rule 41.33 addresses the informality noted in the February 23, 2007 Final Office Action.

2) Rejection under 35 U.S.C. 102(e) over U.S. Publication 2003/0046238 to Nonaka

Claims 36-40:

To illustrate that Nonaka merely discloses a conventional revocation scheme rather than the claimed file-by-file revocation scheme, consider the following background for Nonaka: As discussed with regard Figure 1 in ¶179, a user home network 103 includes a "network device" 160₁ and audio-visual machines 160₂ through 160₄. All of these networked devices include a "secure application module" (SAM). The network device receives a "secure container"

file 104 from a content provider 101. To gain access to the encrypted content within the secure container, the network device interfaces with an "EMD service center" 102. The secure container may be received over the Internet or may be received offline in a storage medium as shown in Figures 11 – 16.

Any revocation discussed in Nonaka would be with regard to the entire secure container and not to specific files within the secure container. Instead, as described in ¶671 of Nonaka, revocation is between the SAMs. Specifically, "in performing communication between the SAMs, each SAM checks the revocation list for whether the corresponding SAM has become invalid, in which case, the communication therebetween is discontinued." Although Nonaka never explicitly addresses the issue, it is evident that this revocation check occurs during the "mutual authentication" of the corresponding SAMs as discussed, for example, in ¶516, which concerns the playback of content in one of the audio/visual SAMs as governed by the network device SAM.

In that regard, the Applicants readily agree with the Examiner that ¶435 of Nonaka discusses the inclusion of a revocation file within the SAM: but that revocation list applies to the entire content of the SAM – there is absolutely no teaching or suggestion within ¶435 of Nonaka for a file-by-file revocation scheme. The citation to ¶¶ 671-675 of Nonaka adds nothing further: this paragraphs merely refer to the EMD service center updating the revocation lists.

Applicants note that these arguments were presented in the response of November 28, 2006 but were deemed non-persuasive in page 3 of the February 23, 2007 Final Office Action because Applicants' "argument distinguishing the host device of the claimed invention from the cited reference is unpersuasive, especially since Applicant notes such a host device may be personal computer (response p. 4) or 'any physical device that embeds an engine (spec p. 22, line 28).'" Although Applicants dispute that the "SAMs" in Nonaka represent either a host device or storage device, such a dispute is immaterial to the fundamental flaw of Nonaka: it is a merely a conventional "all or nothing" revocation scheme as to the content within the SAM. Indeed, consider Figure 3a of Nonaka, which shows the SAM having "content data" C. This content is further shown in Figure

4. No suggestion exists whatsoever in Nonaka as the revocation of individual files within this content: instead, a Nonaka user is either revoked with regard to all the content in the SAM or not, a classic "all or nothing" revocation that is tightly coupled with authentication. In contrast, claim 36 provides a much more flexible and granular file-by-file revocation scheme by including, for example, the acts of ""reading a revocation list associated with the file from the storage medium, the revocation list containing at least one rule, the at least one rule associating data in the revocation list with data in the certificate; applying the at least one rule on the data in the revocation list and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request." Accordingly, claim 36 and its dependent claims 37-40 are allowable over the Nonaka reference.

On page 2 of the February 23, 2007 Final Office Action, Applicants were "reminded that optional or conditional elements do not narrow the claims because they can always be omitted" and also given a citation to MPEP 2106 II C as support.

Applicants respectfully note that there is no statutory bar to the use of conditional limitations in claims. Indeed, Applicants observe that conditional limitations are commonplace in issued U.S. claims – a perusal of the USPTO database will reveal thousands and thousands of U.S. patents that contain conditional limitations prefaced with "if." In that regard, consider a typical flowchart for a method – most methods will have some sort of conditional node where if condition A exists, the method proceeds with a first course of action and where if condition B exists, the method proceeds with a second course of action. It would be rather curious indeed that U.S. patent law would embrace the patentability of methods but then reject the vast subset of methods that contain conditional acts.

But a conditional limitation is not an optional step: consider the limitation that was deemed to not limit claim 36:

if the application of the at least one rule provides a failing result,
denying the file request

This denial of the file request is mandatory: if the application of the at least one rule provide failing result, the file request must be denied – there is no option of not performing this denial whatsoever. In that regard, claim 36 does not say “if the application of the at least one rule provides a failing result, *perhaps* denying the file request.” There is no optional limitation such as perhaps, maybe, etc. in claim 36. Applicants readily agree that a conditional limitation is being recited – but the claim require acts that determine whether the “if” limitation is satisfied: it is not an option to determine whether the application of the at least one rule provides a failing request because claim 36 demands this determination. And if the application provides a failing result, the denial of the file request follows. Thus, Applicants respectfully submit that it was clear legal error to assert that claim 36 includes optional or conditional elements that did not narrow the claim.

Conclusion

Therefore, in light of the foregoing arguments, Applicants respectfully request the Honorable Board of Appeals to reverse the decision of the Examiner with respect to claims 36 – 40.

Respectfully submitted,

Date: 5/23/08

By: _____


Jonathan W. Hallman
Reg. No. 42,622

Claims Appendix

36. A method of revoking a host device on a file-by-file basis, comprising:
 - receiving at a storage engine a certificate from the host device, the certificate containing a digital signature;
 - authenticating the digital signature;
 - establishing a secure session by transmitting a session key to the host device; and
 - during the secure session:
 - receiving at the storage engine a file request from the host device, the file request being directed to a file stored on a storage medium accessible to the storage engine;
 - reading a revocation list associated with the file from the storage medium, the revocation list containing at least one rule, the at least one rule associating data in the revocation list with data in the certificate;
 - applying the at least one rule on the data in the revocation list and the associated data in the certificate; and
 - if the application of the at least one rule provides a failing result, denying the file request.
37. The method of claim 36, wherein the at least one rule comprises a plurality of rules.
38. The method of claim 36, wherein the storage medium is an optical disk.
39. The method of claim 36, wherein the application of the at least one rule act comprises matching the data in the revocation file with the data in the certificate.
40. The method of claim 36, further comprising: if the application of the at least one rule provides a successful result, granting the file request.

Evidence Appendix

No evidence was submitted under Rules 130, 131, or 132.

Related Proceedings Appendix

There are no related proceedings.